Privacy Laws & Practices for Government Agencies

- Debra Castanon, Privacy Specialist

  California Office of Privacy Protection
- Colleen Pedroza, Chief ISO

  California State Information Security Office

Overview

- Privacy in Government
  - Privacy Principles, Laws, Recommended Practices
- Information Security in Government
  - Standards, Best Practices, Resources

A California Identity Theft Summit

Protecting Privacy Online

Privacy in Government

Managing Personal Information
Responsibly (and Legally)

California Office of Privacy Protection

- Created by legislation, started in 2001
- Mission: Protect consumer privacy by identifying privacy problems and facilitating the development of fair information practices.

COPP Functions

- Consumer assistance
- Information and education
- Law enforcement coordination
- Best practice recommendations

Key Points

- Basic Privacy Principles
- Government Privacy Laws
  - –Information Practices Act
  - –Privacy Policies
  - –SSN Confidentiality Act
  - –Breach Notice
- Recommended Practices

Fair Information Practice Principles (FIPs)

- Transparency
- Collection Limitation
- Purpose Specification
- Use Limitation
- Data Quality
- Individual Participation
- Security
- Accountability

Federal Govt. Privacy Laws

- Privacy Act of 1974
  - Based on FIPs
- E-Government Act of 2002
  - Privacy Impact Assessments
  - Web site privacy notices (P3P)

State Govt. Privacy Laws

- Information Practices Act of 1977
  - Civil Code § 1798 et seq.
  - Includes Breach Notice Law § 1798.29
- Social Security Number Confidentiality
  - Civil Code § 1798.85-1798.86
- State Agency Privacy Policies
  - Government Code § 11019.9

Gaps in the Govt. Privacy Regime

	Federal Govt	State Govt	Local Govt
Open public records	Yes	Yes	Yes
Personal info protected	Yes	Yes	**NO**
SSN protected	Yes	Yes	Yes
Security breach notification	Yes	Yes	**NO**

Information Practices Act

- State agencies must:
  - Protect personal info from unauthorized, access, use, disclosure, modification.
    - "Personal info" broadly defined
    - Personal info redacted on public records released
  - Provide notice on collection of personal info
  - Make someone responsible for compliance with requirements

State Agency Privacy Policies

- Agencies must enact and post privacy policy statements in offices and on Web sites.
- Agencies must make someone responsible for compliance with policy.

SSN Confidentiality Act

- Prohibits public posting or display of SSN
  - Don’t print SSN on ID/membership cards.
  - Don’t mail documents with SSN to individual, unless required by law.
  - Don’t send in email unless encrypted.
  - Don’t require for Web site log-on unless add’l PW.
- Applies to any “person or entity”

Breach Notification Act

- Must notify people promptly if personal information is acquired by unauthorized person
- Personal info triggering notice:
  - First name or initial and last name, plus
  - SSN, or DL#, or financial account number.

Breach Notification Act

- Triggered by unencrypted, computerized data
- Time allowed for
  - internal analysis to determine scope, and
  - law enforcement investigation

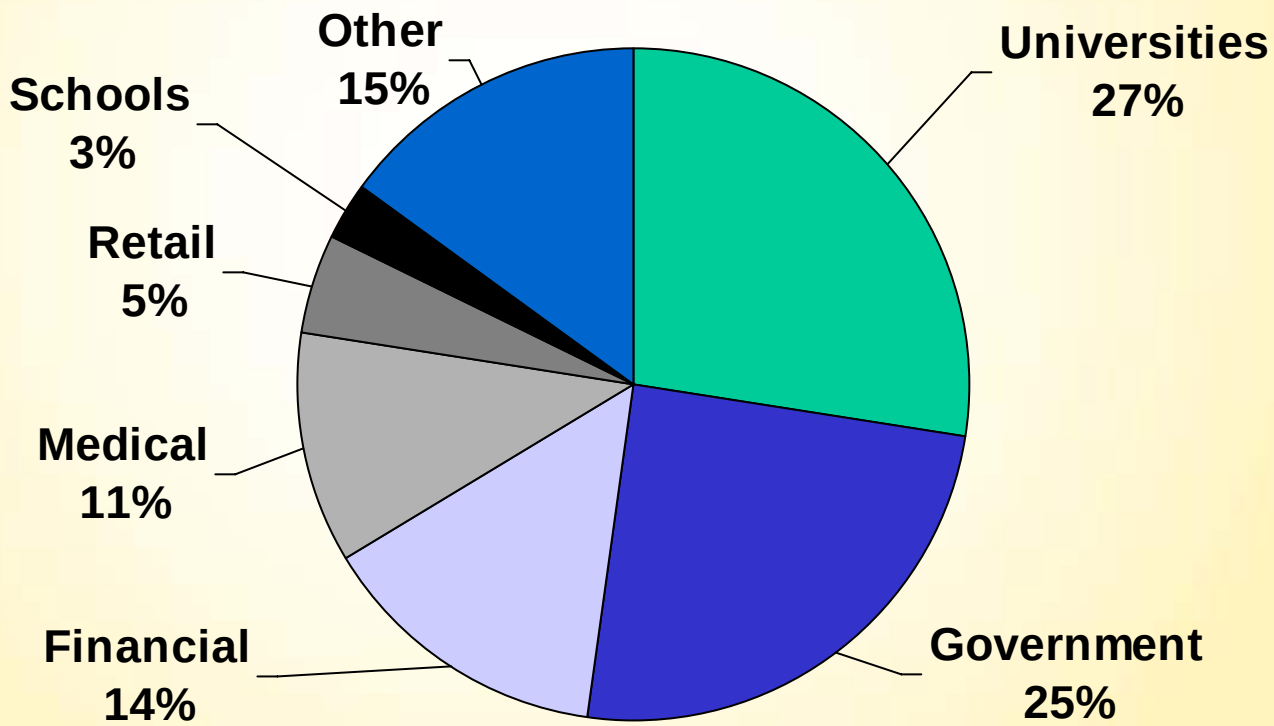
Security Breach Notice

- Notice may be:
  - Written, or
  - Electronic, or
  - Substitute if >$250,000 or >500,000 people
- Substitute notice must be all of:
  - Email when agency has addresses
  - Web site posting
  - Major statewide media

Security Breaches

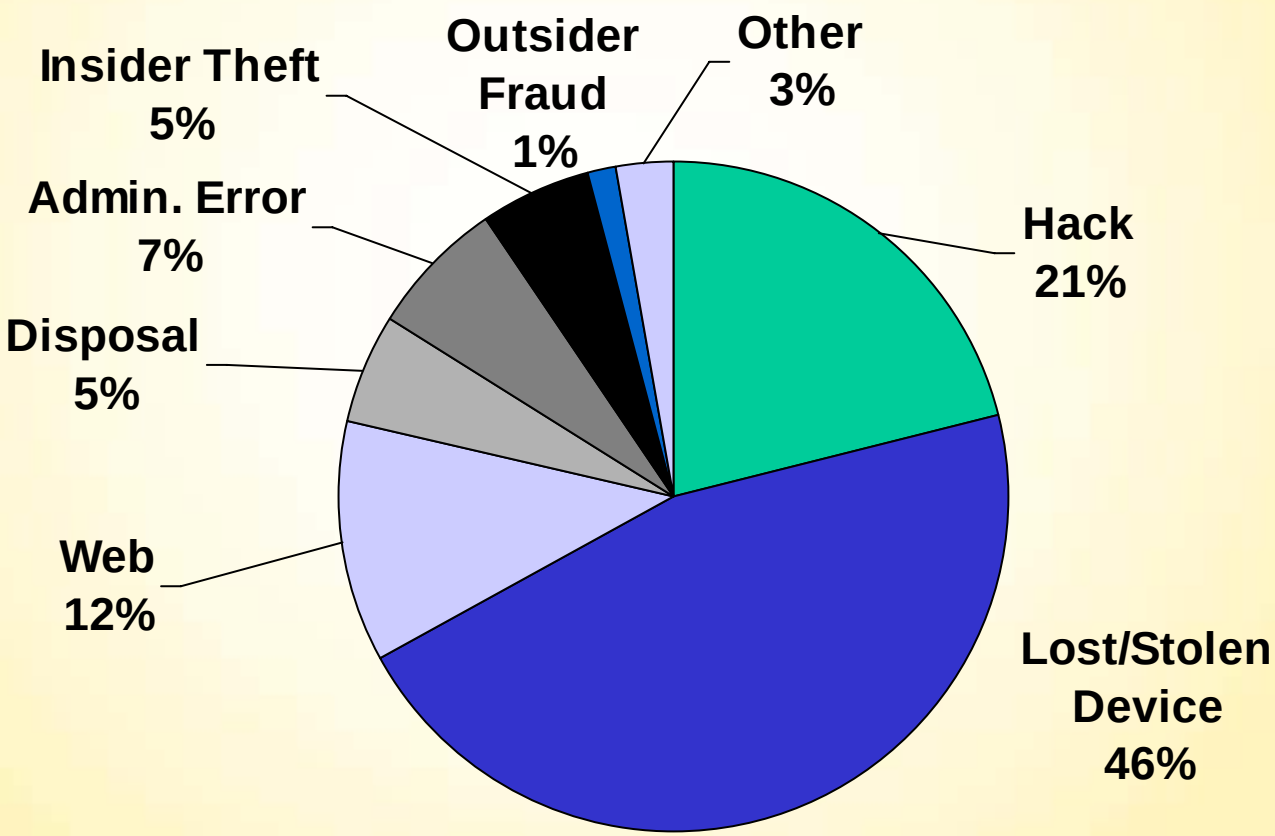
- COPP learns of breaches from consumers who receive notices, companies, state agencies, other organizations, also news media
- Offer assistance (Reco Practices, Call Center FAQs), share lessons learned
- Reviewed sample of 537 breach notifications since 2003

Type of Organization



n=537

Type of Breach



n=537

Lessons Learned from Breaches

- Data retention
  - Universities
- Data collection
  - Blood banks
  - “Personal information is like toxic waste…”
- Limit or protect data on portable devices
  - State agency encryption policy
- Privacy/security awareness training

Pending Legislation

- AB1168 (Jones)
  - What does it change and who is affected?
  - SSNs in Higher Education
  - Public Records including local agencies
  - FTB

Privacy Resources for Government Agencies

- Pending California Privacy Legislation
  - www.privacy.ca.gov/califlegis.htm
- California Privacy Laws
  - www.privacy.ca.gov/lawenforcement/laws.htm
- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
  - www.whitehouse.gov/omb/memoranda/m03-22.html

INFORMATION FOR STATE GOVERNMENT

This page provides resources for California state government agencies on privacy practices and policies for protecting personal information.

- Protecting Privacy in State Government, Basic Training for State Employees
  - PowerPoint Presentation
  - Self-Training Manual *(PDF)*
  - Guidelines for Self-Training Manual *(PDF)*

- Data Classification and Privacy Inventory
  These materials were provided to departmental Information Security Officers and others at workshops conducted in November 2005.
  - Training-PowerPoint Presentation
  - Privacy Inventory Worksheet *(Miscrosoft Excel)*
  - Privacy Inventory Instructions *(PDF)*

- Information on Security Breach Notification
  - Security Incident Notification Steps - State Information Security Office
  - Breach Response Call Center FAQs *(Microsoft Word)*
  - Security Breach Notice Recommended Practices (including Sample Notices) *(pdf)*
  - Security Breach First Steps (One-Page Notice for Breaches Involving Social Security Numbers Only)
    www.privacy.ca.gov/financial/sbfs021205.pdf (English)
    www.privacy.ca.gov/financial/sbfs090404sp.pdf (Spanish)

- California Office of Privacy Protection Recommended Practices
  - Social Security Number Confidentiality *(pdf)*
  - Security Breach Notice *(pdf)*

COPP State Government Web Page: www.privacy.ca.gov/state_gov/index.html

A California Identity Theft Summit

Protecting Privacy Online

Information Security in Government

Safeguarding Privacy with Information Security

CA State Information Security Office (SISO)

- Our Vision
  - Leading the way to secure the State's information assets.
- Our Mission
  - To manage security and operational recovery risk for the State's information assets by providing statewide direction and leadership.

CA SISO Security Program

- Policy
  - Developing, issuing, and maintaining statewide policy, standards, and guidelines
- Assistance/Advisory
  - Providing assistance and advice
  - Providing training and education
  - Providing tools, templates, and samples
- Compliance
  - Ensuring statewide compliance through monitoring, reviews, and audits

Key Points

- Establishing an Effective Information Security Program for Your Organization
- Best Practices for Employees
- Resources

Major Components of a Security Program

- Risk Management
- Policy Management
- Personnel Security
- Privacy
- Physical and Environmental Protection
- System and Communications Protection
- Operations Management
- Access Control
- Security Awareness and Training
- Governance
- Compliance

Risk Management

The process of identifying risk, assessing it, and taking steps to reduce it to an acceptable level.

Organizations should:

- Assign an individual to be responsible for risk assessment.
- Identify information assets, categorize and prioritize them based upon criticality.
- Conduct routine risk assessments.
- Select and implement cost effective protective measures.
- Document results.

Policy Management

Practices and methods used to create and maintain policies to communicate management's position on security principles

Organizations should:

- Further define with standards, guidelines, and procedures.
- Create process for adopting and reviewing policies.
- Clearly identify what can be performed, stored, accessed and used.
- Review periodically or when changes occur.
- Disseminate appropriately.

Personnel Security

Practices, technologies, and services to ensure authorized individuals have appropriate clearances

Organizations should:

- Conduct appropriate background checks.
- Remove access immediately for departed employees/ contactors.
- Create forms and instructions for property use, employee transfers, and terminations.
- Provide specific requirements on use and access for outside entities.

Privacy

Be vigilant in protecting personal, sensitive, or confidential information regardless of media type

Organizations should:

- Secure information through appropriate security measures.
- Limit access to authorized individuals only.
- Ensure incidents are reported immediately.
- Notify affected individuals promptly when incidents occur.
- Provide annual training to all employees and contractors.
- Ensure ongoing audit and evaluation processes are in place.

Physical and Environmental Protection

Practices, technologies, and services used to address threats, vulnerabilities and counter measures utilized to protect information assets

Organizations should:

- Locate system components in a controlled area.
- Implement physical and software controls for portable computing devices.
- Ensure badges and access codes are promptly deactivated as employees/contractors depart.
- Regularly test devices and backup power.

System and Communications Protection

Key elements used to assure data and systems are available and exhibit confidentiality and integrity

Organizations should:

- Deploy appropriate anti-virus and anti-spyware.
- Deploy IDS/IPS solutions.
- Deploy firewalls and other perimeter protection mechanisms.
- Deploy cryptographic solutions for confidential and personal data.
- Not place confidential or personal data in the DMZ.

Operations Management

Implement appropriate controls and protections on IT resources and evaluate threats and vulnerabilities

Organizations should:

- Implement an appropriate level of security monitoring.
- Perform reviews of audit trails on a regular basis.
- Decrease threat of unintentional errors or unauthorized access.
- Separate duties to prevent single control issues.
- Have in place ORPs, security policies, and procedures.

Access Control

Process of controlling access to systems, networks, and data based on business and security requirements

Organizations should:

- Establish formal process for data owners to authorize access.
- Audit access level rights.
- Apply access method of “least privilege.”
- Use a login banner to display conditions of use.
- Restrict connection time to appropriate business hours.
- Initiate automatic logout or protected screen savers.

Security Awareness and Training

Promotes awareness and responsibilities related to the use and management of an organization's information resources.

Organizations should:

- Inform users about policies and procedures.
- Require users to sign acceptable use statements annually.
- Train users to quickly identify threats, how to respond to incidents, and who to contact.
- Use different techniques like posters, email messages, formal instruction, videos, newsletters, and security awareness days.
- Regularly review and update training content to reflect changes.

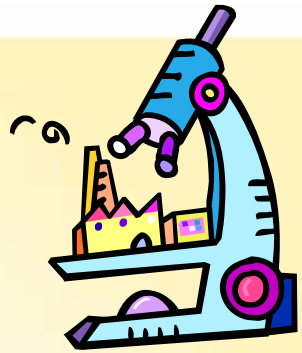
Governance

Enables the enterprise to take full advantage of its information to maximize benefits and capitalize on opportunities

Generates significant benefits including:

- Achieving consensus in the organization.
- Increased predictability and reduced uncertainty of business operations.
- Protection from increasing potential for civil or legal liability.
- Improving trust in customer relationships.

Compliance



Framework for ensuring conformity to applicable security policies and verifying adherence to reporting requirements, including:

- Laws and regulations affecting your organization (HIPAA, etc.)
- Reporting requirements for your organization.
- Promptly investigate and report security incidents.
- Provide notifications when personal identifiable information is breached.

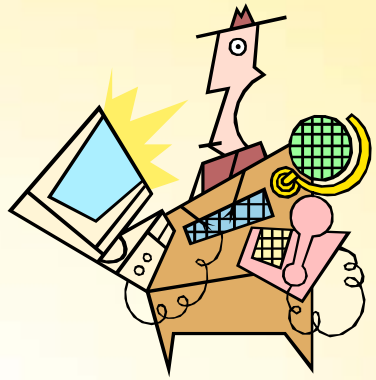
Best Practices

- Executives
- Managers and Supervisors
- IT Staff
- Employees and Contractors

Executives

- Promote information security. It starts at the top!
- Designate an Information Security Officer.
- Recognize that security is a business enabler.
- Make training mandatory for all employees and contractors.
- Develop, update, and review information security policies annually.

Managers and Supervisors



- Realize the value of your organization's information and its reputation.
- Ensure your employees follow policy and good security practices.
- Involve your ISO in all IT projects.
- Know how to recognize a security problem and when to report it to your ISO.
- Inform contractors of security requirements.
- Don't allow untrained staff to take responsibility for securing important systems.

IT Staff

- Report security incidents to your ISO immediately!
- Update anti-virus, spyware, and operating software daily (automate, if possible).
- Conduct an annual security review.
- Complete incremental backups daily, full backups and off-site storage weekly.
- Test your Operational Recovery Plan at least annually.

Employees and Contractors

- Report security incidents to your ISO immediately!
- Read and comply with your organization's security and privacy policies.
- Lock your computer before you leave your seat.
- Use encryption software on your mobile devices, like laptops and personal assistance devices.
- Do not share your passwords.

Cornerstones for Success

- Obtain management support and commitment
- Define roles and responsibilities
- Establish policy, standards, and guidelines
- Develop an effective training awareness program
- Involve other critical offices in your plan
- Monitor and verify compliance

Security Resources

- CA State Information Security Office - www.infosecurity.ca.gov/library/
- CA Office of Privacy Protection – www.privacy.ca.gov/state_gov
- SANS Institute - www.sans.org
- National Institute of Standards and Technology –
  - http://csrc.nist.gov/publications/nistpubs/
    - **NIST Special Publication 800-50** - "Building an Information Technology Security Awareness and Training Program
  - http://csrc.nist.gov/ATE
- United States Computer Emergency Readiness Team (US-CERT) www.us-cert.gov/

Contact Information

Debra Castanon, Privacy Specialist
CA Office of Privacy Protection
Web: www.privacy.ca.gov
Phone: 866-785-9663

Colleen Pedroza, Chief ISO
CA State Information Security Office
Phone: (916) 445-5239
E-Mail: security@dof.ca.gov
Web: www.infosecurity.ca.gov